UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Tecnura
http://revistas.udistrital.edu.co/ojs/index.php/Tecnura/issue/view/650
DOI: http://dx.doi.org/10.14483/udistrital.jour.tecnura.2015.3.a06

INVESTIGACIÓN

WEP, WPA and WPA2 encryption protocols vulnerability on wireless networks with Linux platform

Vulnerabilidad de protocolos de encriptación WEP, WPA y WPA2 en redes inalámbricas con plataforma Linux

Wilmer Antonio Méndez Moreno[1], Darin Jairo Mosquera Palacios[2], Edwin Rivas Trujillo[3]

Fecha de recepción: 12 de febrero de 2014 **Fecha de aceptación:** 18 de agosto de 2015

Cómo citar: Méndez Moreno, W. A., Mosquera Palacios, D. J., & Rivas Trujillo, E. (2015). WEP, WPA and WPA2 encryption protocols vulnerability on wireless networks with Linux platform. *Revista Tecnura*, 19, 79-87. doi: 10.14483/udistrital.jour.tecnura.2015.SE1.a06

Abstract

During the development of telecommunications, several encryption algorithms have been adopted and applied to wireless networks. In operating systems such as Linux, the tools for data transmission over wireless networks are reaching a level of sophistication in reference to other widespread operating systems that are supported by the manufacturers. Thus, designers of protocols for different operating systems, especially Linux, have made every effort to improve the shortcomings of the encryption algorithms. This article analyzes the performance of encryption algorithms which work on the protocols WEP, WPA and WPA2 to provide an overview of how and why wireless protocols and encryption protection must achieve a more scientific basis to detect and prevent attacks , in order to meet the shortcomings associated with encryption algorithms that are currently present.

Keywords: *Wireless Security, WEP, WPA, WPA2, 802.11i, 802.11X*

Resumen

Durante el avance de las telecomunicaciones, se han adoptado varios algoritmos de encriptación aplicados a las redes inalámbricas. En sistemas operativos como Linux, las herramientas para transmisión de datos en redes inalámbricas están alcanzando su nivel de perfeccionamiento en referencia a otros sistemas operativos más difundidos que cuentan con el soporte de los fabricantes. Por ende, los diseñadores de protocolos para diferentes sistemas operativos, en especial Linux, han desplegado todo su empeño en mejorar las falencias de los algoritmos de encriptación. En este artículo son analizados el funcionamiento de los algoritmos de cifrado sobre los cuales funcionan los protocolos WEP, WPA y WPA2 con el fin de proporcionar una visión de cómo y por qué protocolos inalámbricos de protección y cifrado deben lograr una base más científica para detectar y prevenir ataques, con el fin de suplir las falencias asociadas a los algoritmos de encriptación que se presentan en la actualidad.

Palabras Clave: *Seguridad inalámbrica, WEP, WPA, WPA2, 802.11i, 802.11X*

[1] Ingeniero en Telemática de la Universidad Distrital Francisco José de caldas. Bogotá, Colombia. Contacto: wilmermen@gmail.com
[2] Ingeniero de sistemas, magíster en telemática, docente e investigador de la Universidad Distrital Francisco José de Caldas, Bogotá, Colombia. djmosquerap@udistrital.edu.co
[3] Ingeniero electricista, magíster en sistemas de generación de energía eléctrica, máster en ingeniería eléctrica, electrónica y automática, doctor en ingeniería eléctrica, electrónica y automática; docente e investigador de la Universidad Distrital Francisco José de Caldas, Bogotá, Colombia. erivas@udistrital.edu.co

INTRODUCCIÓN

La comunicación inalámbrica es el proceso de comunicar información en los medios electromagnéticos sobre una distancia a través del entorno de espacio libre, en vez de a través de cable tradicional u otros conductos físicos.

La comunicación moderna por red inalámbrica esencialmente comenzó en 1997 con el estándar original 802.11. En 1999, de Protección de equivalencia a cableado (WEP) fue presentado como el primer intento de un algoritmo de seguridad para redes inalámbricas. En 2001 se encuentran defectos graves de seguridad en WEP. Wi-Fi Protected Access (WPA) fue introducido en 2003 como una medida provisional que remplazó WEP, y fue seguido rápidamente por WPA2 en 2004, que aplicó plenamente el estándar 802.11i.

La figura 1 muestra la evolución de las normas inalámbricas desde 1999 hasta la actualidad.

Con el auge de las comunicaciones móviles, las redes inalámbricas se han popularizado, gracias a sus ventajas comparativas, referentes a movilidad, escalabilidad y facilidad de instalación con respecto a las redes convencionales. Además, en la actualidad están pasando por un proceso de innovaciones rápidas, una mayor competencia y la diversidad en la oferta de servicios que genera una reducción de los precios para los consumidores y las empresas. Sin embargo, la información que se transmite a través de estas redes presenta una alta vulnerabilidad en comparación con las redes de cable convencionales dado que el espectro electromagnético por el cual se transmite la información se encuentra expuesto a agentes externos.

Por ejemplo, la comunicación inalámbrica puede ser perturbada por las ondas de radio, una tormenta eléctrica o bloqueada por objetos físicos, como montañas, rascacielos. Incluso peor, puede ser fácilmente atacada por virus informáticos, aparatos de espionaje y amenazas similares. En las comunicaciones inalámbricas la autenticación y el cifrado de datos (criptografía) son las áreas de interés.

Los organismos de normalización y fabricantes están gastando enormes cantidades de dinero y tiempo en el desarrollo y despliegue de soluciones de próxima generación frente a los crecientes problemas de seguridad de red inalámbrica, lo que ha motivado que la comunidad científica trabaje en pro de nuevos desarrollos para la comunicación en redes inalámbricas bajo la bandera de Linux.

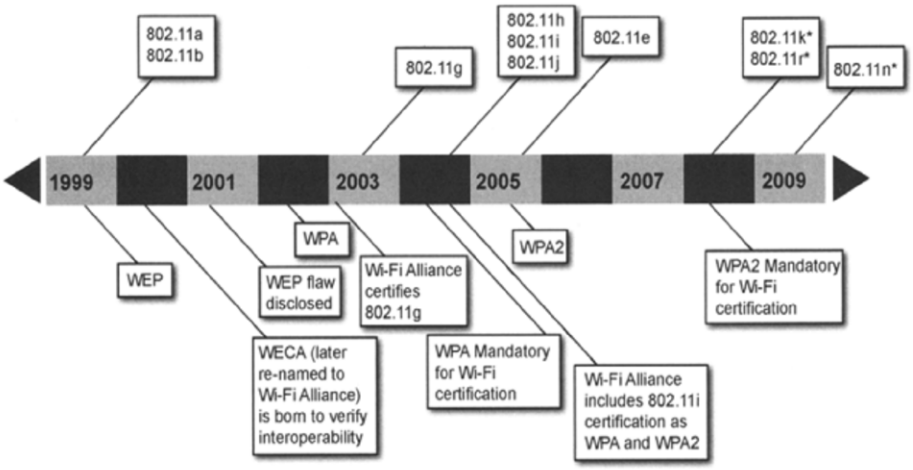

Figura 1. Línea de tiempo de la evolución de las normas inalámbricas.

(Levy, Tran, et al., 2007, pp. 1-24).

Este artículo se centra en las vulnerabilidades que vienen con las comunicaciones inalámbricas y cómo ello se relaciona con las amenazas y los riesgos.

ESTADO DEL ARTE

Muchos algoritmos de cifrado están ampliamente disponibles en las redes cableadas. Ellos se pueden clasificar en cifrado de clave simétrica y asimétrica. En el cifrado de clave simétrica o cifrado de clave secreta solo se utiliza una clave para encriptar o cifrar y desencriptar o descifrar datos y la clave debe ser distribuida antes de la transmisión entre las entidades. Se sabe que es muy eficiente ya que el tamaño de la clave puede ser pequeño, las funciones utilizadas para la encriptación son operaciones de hardware, y el tiempo de cifrado puede ser muy rápido. Sin embargo, en las redes de comunicación de gran tamaño, la distribución de la clave puede ser un problema significativo. El cifrado de clave asimétrica o el cifrado de clave pública se utiliza para resolver el problema de distribución de claves. Este utiliza dos claves, una para encriptación y otra para desencriptación, y no es necesario para la distribución de ellas antes de la transmisión. Sin embargo, el cifrado de clave pública se basa en funciones matemáticas, computacionalmente intensivas y no muy eficientes para pequeños dispositivos inalámbricos (Schneier, 1996).

Generalmente, la mayoría de los cifrados utilizados en los dispositivos inalámbricos se basan en el cifrado de claves simétricas. En las redes WLAN (*Wireless Local Area Networks*, redes de área local inalámbricas), la privacidad se consigue mediante la protección de datos con contenido cifrado. El cifrado es opcional en redes WLAN 802.11, pero sin ella cualquier otro dispositivo inalámbrico estándar puede leer todo el tráfico en la red. Hasta el momento existen tres generaciones principales para la seguridad en redes inalámbricas:

- WEP (Wired Equivalent Privacy), es la norma de seguridad 802.11.
- WPA (Wi-Fi Protected Access), es la norma 802.11i.
- WPA2/802.11i (Wi-Fi de Protected Access2).

Un primer intento de la seguridad de WLAN fue el protocolo WEP, desarrollado para proporcionar un modelo de transporte seguro en redes de área local (Nicopolitidis, Obaidat, et al., 2003, Obaidat, and Boudriga, 2007). El algoritmo utiliza el cifrado RC4, el cual es conocido por ser rápido y eficiente; además puede escribirse utilizando solo unas pocas líneas de código y requiere solo 256 bytes de RAM (Schneier, and Whiting, 1997, pp. 242-259).

WEP fue uno de los mejores esquemas de cifrado durante la última década. No obstante, Fluhrer y muchos investigadores han descubierto varias vulnerabilidades en el algoritmo (Fluhrer, Mantin, *et al*. 2001, pp. 1-24, Stubblefield, Ioannidis, Rubin, 2004, pp. 319-332).

Las debilidades en RC4 y en el protocolo WEP dieron lugar a un nuevo estándar para la seguridad en redes WLAN denominado WAP o conocido como TSN (Transition Security Network).

WPA aborda las debilidades de la privacidad de los datos de WEP mediante la incorporación del Protocolo de Integridad de Clave Temporal (TKIP), una implementación mucho más fuerte del algoritmo de cifrado RC4, además de un sofisticado sistema de claves dinámicas que mejora notablemente la privacidad de los datos y funciones de autenticación. En general, WPA es TKIP con IEEE 802.1X (Fluhrer, Mantin, *et al*. 2001, pp. 1-24), el cual se introdujo para tratar específicamente las funciones de autenticación en el entorno de red. El estándar IEEE 802.1X mejora el estándar IEEE 802.11i, con su potente autenticación, autorización, y las funciones de gestión de claves.

WPA puede ser violentado, es decir, se puede descubrir la clave cifrada a través de varios métodos; uno de ellos es un ataque de fuerza bruta con la herramienta Aircrack, la cual requiere un diccionario de posibles claves para penetrar la red, dado que WPA introduce mejoras significativas respecto a WEP.

En la actualidad el medio más eficiente de encriptación para redes inalámbricas es WPA2, el cual remplaza el WPA e introduce el CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), para remplazar TKIP (el protocolo obligatorio en el WPA). CCMP proporciona una nueva forma de encriptación más segura basado en el cifrado por bloques AES. Este es un cifrado de bloques diseñado por Joan Daemen y Vincent Rijmen y que tiene una longitud variable clave de 128, 192, o 256 bits para cifrar bloques de datos de 128, 192, o 256 bits de largo. Tanto el bloque como la longitud de clave son extensibles a múltiplos de 32 bits. El cifrado AES es rápido y flexible, y puede ser implementado en varias plataformas, especialmente en dispositivos pequeños y la tarjeta inteligente (MacMichael, 2005). Además, AES ha sido rigurosamente probado para agujeros de seguridad durante algunos años antes de que fuera estandarizado por el NIST. S AE. y se considera muy seguro. Pero Bogdanov, A. *et. al*. (https://lirias.kuleuven.be/bitstream/123456789/314284/1/aesbc.pdf) pretenden demostrar un ataque para recuperar la contraseña sin procesos de fuerza bruta.

METODOLOGÍA

En este apartado se presenta la metodología que han desarrollado organismos de normalización y fabricantes en el proceso de encriptación WEP y WAP.

Proceso de encriptación WEP

En la figura 2 se ilustra el proceso de encriptación WEP, en el cual se genera una llave de 64 o 128 bits a partir de la contraseña introducida para la seguridad de la red. Al tamaño de la llave se le debe restar 24 bits del vector de inicialización, razón por la cual se utiliza contraseñas de 40 o 104 bits, o lo que es igual, 5 o 13 caracteres ASCII, dependiendo de la longitud con que se trabaje (Lashkari, Danesh, Samadi, 2009).

La llave se obtiene a partir de una semilla a través de una operación XOR realizadapor una cadena de caracteres ASCII de 13 bits llamada *Mi Contraseña* escrita por el usuario. En la figura 1 se ilustra cómo a partir de una semilla, un generador aleatorio de números (PRNG) genera automáticamente 40 cadenas de 32 bits cada una. De cada cadena se toma un bit para generar 4 llaves, de las cuales se selecciona una para la encriptación (Lashkari, Danesh, Samadi, 2009).

Con base en el estándar 802.11 para redes inalámbricas, las tramas de la capa dos del modelo OSI contienen una cabecera y los datos. A las tramas se añade a través de un algoritmo llamado CRC un valor de chequeo de integridad o ICV, cuyo propósito es proporcionarle al paquete un identificador único, para verificar que los datos recibidos sean los mismos enviados. El vector de inicialización es un contador, el cual aumenta su valor en la medida en que se envían paquetes. Este vector conjuntamente con la llave seleccionada para encriptación se le aplica el algoritmo RC4, generando un flujo de llave; a este simultáneamente con el paquete de datos se le realiza una operación XOR, obteniendo un paquete de datos encriptado. Este último se concatena nuevamente con el vector de inicialización y la llave, quedando la trama completa.

En una red en donde exista un gran número de flujo de paquetes, el vector de inicialización se puede agotar rápidamente debido a que solo hay disponibles 2^{24} posibilidades de envío de tramas. Esto origina que sea fácil detectar la clave de la red, provocando que sea vulnerable la seguridad de la misma (Lashkari, Danesh, Samadi, 2009).

Debilidades de WEP

WEP tiene muchas debilidades asociadas, entre las cuales se destacan (Arash Habibi Lashkari, Towhidi, Hoseini, 2009):

- WEP no impide la falsificación de paquetes.
- WEP no previene los ataques de repetición. Un atacante puede simplemente grabar y reproducir

los paquetes como se desee y serán aceptados como legítimos.

- WEP utiliza incorrectamente RC4. Las claves utilizadas son muy débiles, y pueden ser violentadas usando software libre.
- WEP reutiliza vectores de inicialización. Diversos métodos disponibles pueden descifrar los datos sin conocer la clave de cifrado.
- WEP permite a un atacante modificar imperceptiblemente un mensaje sin conocer la clave de cifrado.

Proceso de encriptación WPA y WPA2

El proceso de encriptación de WPA se ilustra en la figura 3. En la primera fase se genera una cadena de caracteres con el password, la dirección MAC del emisor, y el vector de chequeo de inicialización. La dirección MAC es incorporada en la cadena de caracteres del emisor del mensaje, permitiendo que no se pueda descifrar por extraños. En la segunda fase se añade la llave dinámica seleccionada combinándose con el número de paquetes que se envía (Fluhrer, Mantin, *et al*., 2001, pp. 1-24).

A diferencia de WEP, WPA utiliza en la cabecera de la trama 48 bits para cada paquete transmitido, lo que le permite ser menos vulnerable que su antecesor.

Las claves WPA pueden ser encontradas haciendo un proceso de autentificación de un cliente a una red (handshake); para ello se puede usar búsquedas por fuerza bruta (Arash Habibi Lashkari, Towhidi, Hoseini, 2009), siendo esta una debilidad de la encriptación WPA, la cual puede ser subsanada utilizando claves más elaboradas (Arash Habibi Lashkari, Towhidi, Hoseini, 2009).

En la tabla 1 se muestra la evolución de los sistemas de encriptación inalámbricos con base en el algoritmo, características, longitud de las claves, vulnerabilidad y ataques conocidos.

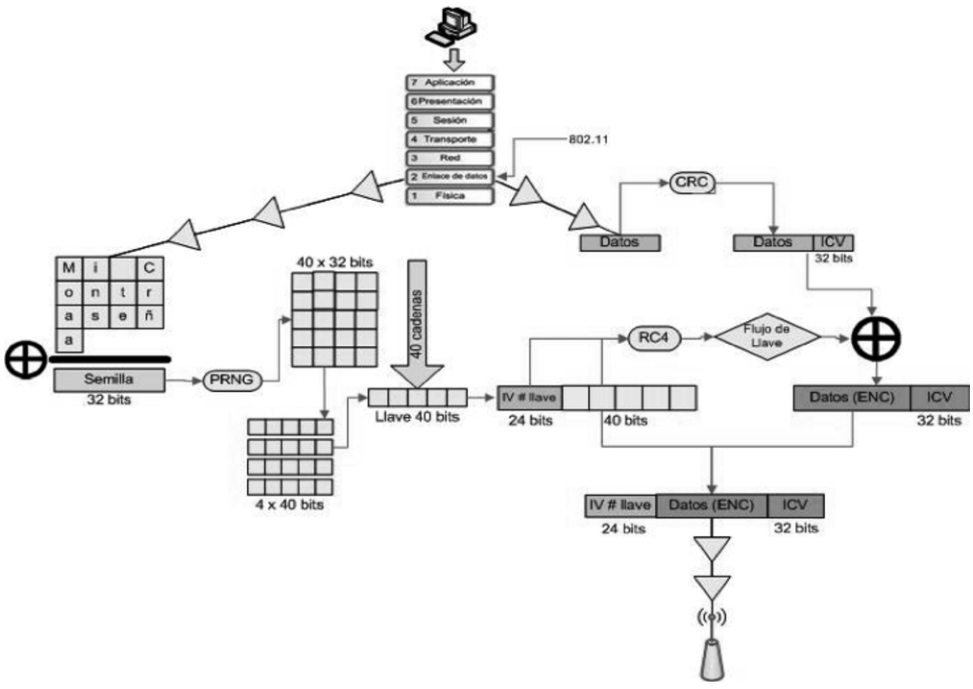

Figura 2. Proceso WEP

Fuente: (Pau Oliva Fora. Inseguridad en redes 802.11b. 2003).

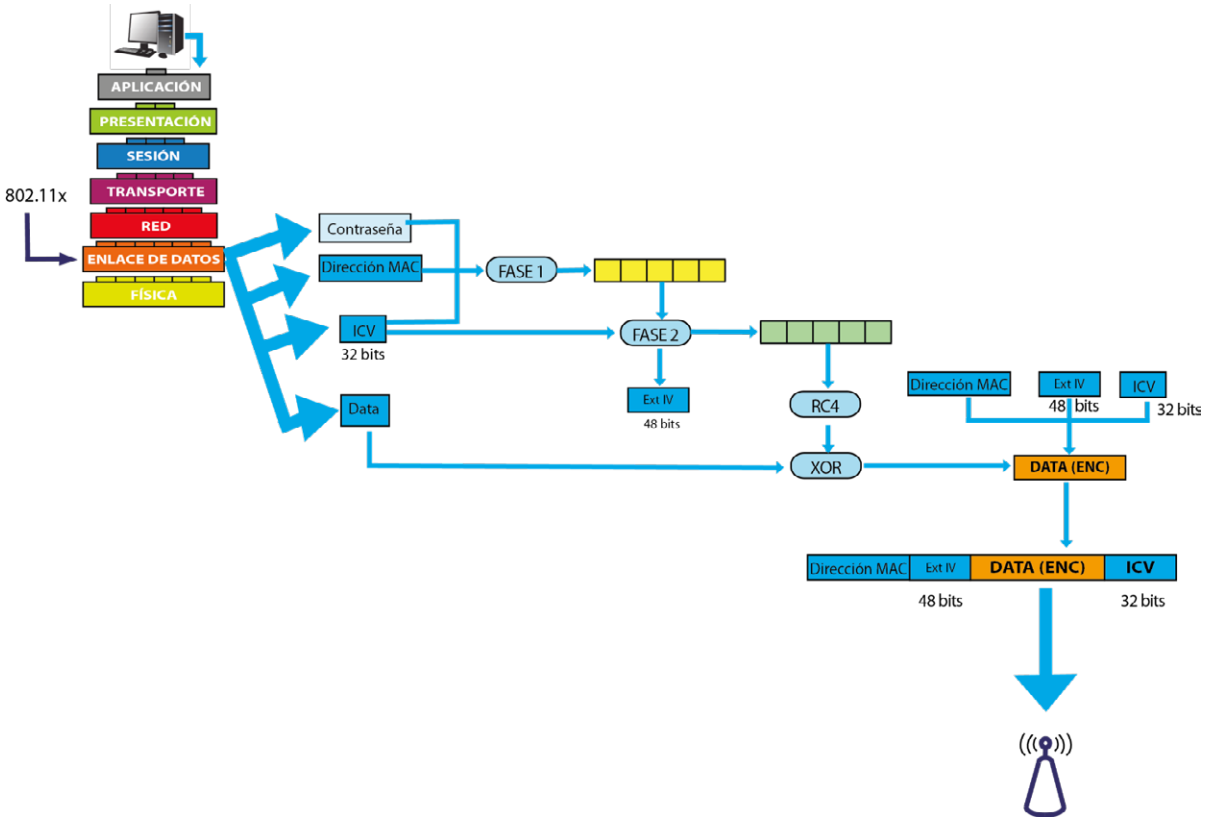

Figura 3. Encriptación WPA

Fuente: (Pau Oliva Fora. Inseguridad en redes 802.11b. 2003).

Tabla 1. Evolución de sistemas de codificación inalámbrica

Sistema de encriptación	**WEP**	**WPA**	**WPA2**
Estándar	802.11b	802.11g	802.11i
Algoritmo	RC4	RC4TKIP	AES (Rijndael)
Características	Protección a redes inalámbricas vulnerables	IV extendido Llaves dinámicas (TKIP) Incluye MAC del emisor	Número algoritmo de mayor complejidad Tramas convertidas por operaciones matriciales
Longitud de claves	**64 (40) o 128 (104) bits**	**128 a 256 bits**	**128 a 256 bits**
Vulnerabilidad	IV muy corto Llaves estáticas Claves cortas Chequeo de integridad independiente de datos cifrados	Autenticación por handshake auditable. Claves en diccionario, o reconocibles por atacante	Claves conocidas Rondas cortas en información muy confidencial Uso de claves en diccionario o conocidas por atacante
Ataques conocidos	FMS, por estadística de IV, muy exitoso, obteniendo gran cantidad de tramas con IV	Por fuerza bruta comparando claves con handshake, éxito dependiente de tener la clave en el diccionario	Por fuerza bruta muy lenta comparando directamente con la red claves de diccionario, muy poco éxito en bastante tiempo de ataque

Fuente: elaboración propia

RESULTADOS

Tasas de transmisión en redes inalámbricas Linux

En la figura 4 se muestra el esquema de conexión de red inalámbrica implementado para la transmisión de archivos entre nodos usando los diferentes sistemas de encriptación.

En la tabla 2 se muestran los resultados obtenidos a partir de un archivo de 10 y 49 MB, respectivamente. Aunque no se encontraron resultados concluyentes respecto a diferencias en los tiempos de transmisión comparando los distintos métodos de cifrado, se observó que la velocidad del canal usado por los dispositivos de conexión inalámbrica de 9 MB no fue usada en su totalidad, es decir, no llega a lo definido por el estándar 802.11g de 54 Mbps (Gurkas, Zaim, and Aydin, 2006, pp. 1-5).

Con las pruebas efectuadas con un tamaño de archivo de 10 MB siempre se obtuvo mayor velocidad de transmisión en equipos con sistema operativo Windows con respecto a los de sistema operativo Linux.

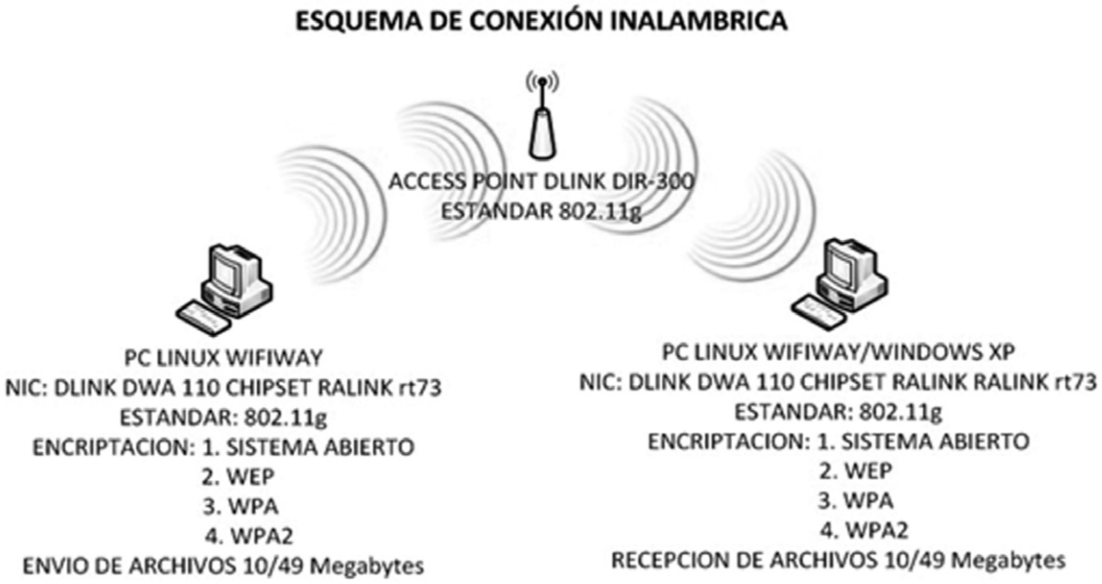

Figura 4. Esquema de conexión de red

Fuente: elaboración propia

Tabla 2. Tasas de transmisión en redes inalámbricas

Protocolos	Archivo de 49 MB	N° de envíos	Archivo de 10 MB		N° de envíos
	Tiempo de transmisión Linux		Tiempo de transmisión Linux	Tiempo de transmisión Linux/Windows	
1. Sistema abierto	25 s	10 trans.	145 s	15 s	20 trans.
2. WEP	1.620 s		310 s	10 s	
3. WPA	1.800 s		360 s	8 s	
4. WPA2	1.380 s		420 s	8 s	

Fuente: elaboración propia

Resultados experimentales

Ante las vulnerabilidades de WEP se han generado aplicaciones para quebrantar su algoritmo de cifrado. Varias de estas herramientas, como Airodump, Aireplay y Aircrack se condensaron en Wifislax y Wifiway, distribuciones sobre Linux creadas específicamente con el objetivo de realizar estudios de la seguridad en redes tanto inalámbricas como cableadas (Arash Habibi Lashkari, Towhidi, Hoseini, 2009).

El principal problema que se presenta al implantar una red inalámbrica en Linux es que los chipset de muchas de las tarjetas de conexión que existen en el mercado no tienen compatibilidad, lo que implica que no existe un controlador para el buen desempeño. Las únicas tarjetas que funcionan en Linux contienen chipsets con código abierto, lo que permite a los desarrolladores generar el respectivo controlador de la tarjeta (Fluhrer, Mantin, *et al*., 2001). Para demostrar las debilidades de la encriptación de WEP con aplicaciones Linux, se capturaron paquetes de un canal determinado almacenándolos en un archivo que contiene los vectores de inicialización con los cuales se hace la búsqueda de la clave.

La aplicación Aireplay realiza ataques a la red para que se transmitan suficientes paquetes de datos ARP lanzados por el cliente legítimamente conectado, esperando que el Access Point responda con paquetes que contienen vectores de inicialización (IV) que son almacenados en un archivo por el software Airodump.

La búsqueda de la clave se hace con los IV capturados en la red. El tiempo promedio para encontrar una clave de 64 bits es 3 a 10 minutos, dependiendo de los datos recopilados y el tipo de caracteres que tenga la clave; una de 128 bits en promedio puede tardar de 20 a 60 minutos en ser hallada con el software Aircrack. Para WPA por ser un protocolo más robusto que WEP se hace más complejo detectar la clave, y para encontrarla se siguen los mismos pasos que se dan para WEP, pero la clave debe encontrarse por fuerza bruta haciendo comparaciones en un diccionario (Gurkas, Zaim, and Aydin, 2006, pp. 1-5).

Para comenzar con el proceso se necesitó un handshake, este se consigue capturando un alto número de paquetes de tráfico WPA en la red. Con los paquetes almacenados, se hace un proceso en donde se comparan palabras de un diccionario hasta encontrar la clave que es compatible con el handshake; este método no es infalible si la red implementa una clave con caracteres especiales que no está en el diccionario (Gurkas, Zaim, and Aydin, 2006, pp. 1-5). Las pruebas que se ejecutaron solo son posibles para WEP y WPA, ya que las herramientas utilizadas solo funcionan con el algoritmo RC4; para el protocolo WPA2 que funciona con el algoritmo AES hasta el momento no existen formas plausibles de hallar las contraseñas.

CONCLUSIONES

Desde la llegada de las redes inalámbricas en 1997, el progreso tecnológico en este campo ha sido enorme. Sin embargo, presenta problemas de vulnerabilidades en la seguridad. WEP estableció un método de protección para datos transmitidos por redes inalámbricas en sus inicios, pero actualmente es insuficiente ya que su algoritmo ha sido descifrado, y es posible romperlo en prácticamente cualquier situación de longitud de claves o uso privado. El sistema WPA ofrece algo más de protección con respecto a WEP, ya que aunque tiene el mismo algoritmo introduce mejoras que hacen un poco más complicado descifrarlo. El ataque a una red WEP o WPA requiere la recolección de gran cantidad de paquetes transmitidos, por lo que no es recomendable su uso en una red que tenga un tráfico alto a no ser que no exista otra opción, debido a que la cantidad de tiempo en que se hallará una clave será menor. WPA2 es el método de encriptar redes inalámbricas más seguro hasta la fecha, ya que su algoritmo es suficientemente complejo y con suficientes precauciones y prácticas de seguridad informática se hace más complicado obtener las contraseñas rápidamente sin ataques de fuerza bruta.

FINANCIAMIENTO

Este proyecto ha sido financiado con recursos propios.

REFERENCIAS

Arash Habibi Lashkari, Towhidi, F., Hoseini, R.S. (2009). Wired Equivalent Privacy (WEP). ICFCC. Kuala Lumpur Conference.

Fluhrer, S., Mantin, I., *et al*. (2001). Weaknesses in the key scheduling algorithm of RC4. In: Eighth Annual Workshop on Selected Areas in Cryptography. Toronto, Canada. Aug.

Gurkas, G. Z., Zaim, A. H., and Aydin, M. A. (2006). Security Mechanisms and their Performance Impacts on Wireless Local Area Networks. International Symposium on Computer Networks, June, pp. 1-5. https://lirias.kuleuven.be/bitstream/123456789/314284/1/aesbc.pdf, abril 13 de 2013.

Lashkari, A.H., Danesh, M.M.S., Samadi, B. (2009). FCSIT. A survey on wireless security protocols (WEP, WPA and WPA2/802.11i). *Computer Science and Information Technology*. ICCSIT. 2nd IEEE International Conference.

Levy, J., Tran, K., *et al*. (2007). Introduction to Secure Wireless Networking.

Sonic WALL Secure Wireless Network Integrated Solutions Guide.

MacMichael, John L. (2005). Auditing Wi-Fi Protected Access (WPA) Pre-Shared Key Mode. *Linux Journal*.

Nicopolitidis, P., Obaidat, M. S., *et al*. (2003). *Wireless Networks*. New York: Wiley.

Obaidat, M. S., and Boudriga, N. (2007). *Security of e-Systems and Computer Networks*. Cambridge, U.K.: Cambridge University Press.

Schneier, B. (1996). *Applied Cryptography.* John Wiley & Sons, Inc.

Schneier, B. and Whiting, D. (1997). Fast Software Encryption: Designing Encryption Algorithms for Optimal Software Speed on the {Intel Pentium} Processor. *Lecture Notes in Computer Science*, vol. 1267.

Stubblefield, A., Ioannidis, J., Rubin, A.D. (2004). A key recovery Attack on the 802.11b Wired Equivalent Privacy Protocol (WEP). *ACM Transactions on Information and System Security*, Vol. 7, No. 2, May.